

AD-A141 490

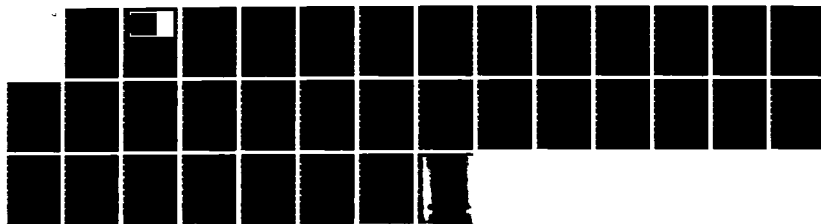
STOCHASTIC MODELS FOR COMMON FAILURES OF COMPONENTS(U)
WISCONSIN UNIV-MADISON MATHEMATICS RESEARCH CENTER
B HARRIS MAR 84 MRC-TSR-2659 DRAG29-80-C-0041

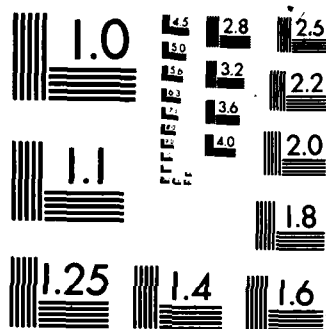
1/1

UNCLASSIFIED

F/G 12/1

NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963 A

AD-A141 490

MRC Technical Summary Report #2659

STOCHASTIC MODELS FOR COMMON FAILURES
OF COMPONENTS

Bernard Harris

Mathematics Research Center
University of Wisconsin—Madison
610 Walnut Street
Madison, Wisconsin 53705

March 1984

(Received December 27, 1983)

DTIC FILE COPY

Approved for public release
Distribution unlimited

Sponsored by

U. S. Army Research Office
P. O. Box 12211
Research Triangle Park
North Carolina 27709



84 05 31 075

UNIVERSITY OF WISCONSIN-MADISON
MATHEMATICS RESEARCH CENTER

STOCHASTIC MODELS FOR COMMON FAILURES
OF COMPONENTS

Bernard Harris*

Technical Summary Report #2659

March 1984

ABSTRACT

Various models for common failures are described and characterized. In particular, a time dependent stress-strength (loading) model is given.

AMS (MOS) Subject Classifications: 62N05, 60K10, 90B25

Key Words: Common failures, dependent failures, common mode failures,
common cause failures

Work Unit Number 4 (Statistics and Probability)

*Appeared as a University of Wisconsin-Madison, Department of Statistics,
Technical Report #727

Sponsored by the United States Army under Contract No. DAAG29-80-C-0041.

SIGNIFICANCE AND EXPLANATION

Much of the literature dealing with system failures assumes that individual subsystems or components are stochastically independent. In this report, some models that have been used for analyzing dependent failures are examined and one new model is proposed. These models are of particular interest in the probabilistic risk assessment of nuclear reactors.

Accession For	
NTIS GRA&I	<input checked="" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	



The responsibility for the wording and views expressed in this descriptive summary lies with MRC, and not with the author of this report.

STOCHASTIC MODELS FOR COMMON FAILURES OF COMPONENTS

Bernard Harris*

1. Introduction

In the probabilistic modeling of problems in systems reliability, the possibility that failures of components may be stochastically dependent is often neglected. In some areas of application, such as the safety of nuclear reactors, the treatment of such dependent failures has been the subject of substantial controversy. This report is primarily motivated by the treatment of dependent failures in the nuclear reliability literature. Nevertheless, the models described herein have quite general applicability.

We begin this discussion with a summary of the various modes of dependent failures, as classified in the nuclear reliability literature. Unfortunately, the terminology is not consistent and the same terms are defined differently by the various writers. Further, the same mathematical model may be an appropriate description of more than one type of dependent failure.

Specifically, a common mode failure is the simultaneous failure of more than one component. In the engineering literature, (see, for example, the PRA Procedures Guide [17]) it is assumed that the failures are not stochastically independent. In the treatment that follows, no assumption about the stochastic independence or lack thereof is made. This is a mathematical convenience, since stochastic independence is a limiting case of stochastic dependence.

*Appeared as a University of Wisconsin-Madison, Department of Statistics, Technical Report #727.

Sponsored by the United States Army under Contract No. DAAG29-80-C-0041.

Additional detailed general discussions of common mode failures and their analyses may be found in Edwards and Watson [7] and the Deutsche Risiko Studie - Kernkraftwerke [10].

A failure of a component or subsystem is said to be a propagating failure when the failure changes the operating conditions, environments or requirements in such a way as to cause the failure of other equipment. Here we will be interpreting this definition in the manner of a classical mathematical model of H. E. Daniels [4], which may be described as follows. Envision a cable consisting of m wires intertwined. This cable is supporting a load and the load is distributed among the m wires. If $1 < k < m$ wires break, then the load is redistributed among the remaining $m - k$ wires, increasing the chance that they will rupture. It is in this sense that one can model propagating failures, that is, the failure of some components increases the stress on others. P. K. Sen [14,15] has studied statistical inference for the model. A failure is said to be a common cause failure if more than one component fails due to a single cause (usually assumed to be external to the operating conditions of the equipment). Such common causes may be earthquakes, fires, floods, volcanic eruptions, or lightning strikes.

Consequently, in modeling common cause failures, it is desirable to introduce point processes for initiating events. Physically, an initiating event is to be regarded as the external occurrence such as a flood, earthquake, power outage, or fire, which can cause the failure of several components simultaneously, due to the environmental stresses occasioned by its occurrence.

Another cause of simultaneous failures of several components occurs when one device has several functions, so that its failure prevents each of these

individual functions from operating. Such might be the case if two cooling tanks were fed by the same water supply pipe. These types of common mode failures are known as shared-equipment dependencies and should be detectable by an examination of the logic diagram of the system. Such possible common mode failures, being dependent on the engineering design of the system, can be avoided by proper design and should not be of concern for this study.

Another possibility which may call for dependent modeling of component lifetimes is the presence of standby components. Such a component is called into use when a specified component or specified components have failed. Thus, it is plausible that a failure may be detected (or may occur, in the case of demands) only after these other components have failed. Consequently, the conditional waiting time until a failure in the standby component is observed is different from the waiting time until failure if it were in primary (non-standby) usage.

In Section 2, the square root bounding method is discussed. This method was introduced in WASH-1400 [16] and has been severely criticized. The beta factor model is described in Section 3. The common load model of Mankamo [12,13] is described in Section 4. In Section 5, the binomial failure model (see Veseley [18]) is introduced and in Section 6, a shock model of Apostolakis [1] is defined. A model proposed by the author is presented in Section 7. The square root bounding method, the beta factor model and the binomial failure rate model are compared in Fleming and Raabe [9]. Concluding remarks are given in Section 8.

2. The Square Root Bounding Method.

The highly controversial method discussed in this section was introduced in WASH-1400 [16, Appendix IV].

Let $A_i, i = 1, 2, \dots, m$ be a finite sequence of events. The authors of WASH-1400 wished to obtain a convenient approximation to $P(\bigcap_{i=1}^m A_i)$. This approximation should be sufficiently simple to permit statistical estimation or to facilitate computation, or capable of determination from prior knowledge of the properties of the events A_i , or from engineering judgment.

In WASH-1400, because of the intended application, it is assumed that the events A_i denote failures of components or subsystems.

We now describe the square root bounding method. Trivially, we have

$$P(\bigcap_{i=1}^m A_i) \leq P(\bigcap_{i \neq j} A_i), \quad 1 \leq j \leq m \quad (2.1)$$

Let C_1 and C_2 be arbitrary subsets of $\{1, 2, \dots, m\}$. Then, in view of the intended application, we assume

$$P(\bigcap_{i \in C_1} A_i \mid \bigcap_{j \in C_2} A_j) \geq P(\bigcap_{i \in C_1} A_i). \quad (2.2)$$

Thus, (2.2) expresses the assumption that the failure of some components will not decrease the probability of the failure of other components.

One employs (2.1) and (2.2) to obtain upper and lower bounds to $P(\bigcap_{i=1}^m A_i)$. We denote these bounds by $\bar{P}(\bigcap_{i=1}^m A_i)$ and $\underline{P}(\bigcap_{i=1}^m A_i)$ respectively. Thus,

$$\underline{P}(\bigcap_{i=1}^m A_i) \leq P(\bigcap_{i=1}^m A_i) \leq \overline{P}(\bigcap_{i=1}^m A_i) \quad (2.3)$$

and the approximation proposed in WASH-1400 is

$$\tilde{P}(\bigcap_{i=1}^m A_i) = (\overline{P}(\bigcap_{i=1}^m A_i) \underline{P}(\bigcap_{i=1}^m A_i))^{1/2}, \quad (2.4)$$

hence the name "square root bounding method."

The precise selection of the bounds appears to be not completely prescribed by WASH-1400 and subsequent writing on this procedure. However, the following appears to be the most commonly employed choice.

Example 2.1 From (2.1), it follows by induction that

$$P(\bigcap_{i=1}^m A_i) \leq \min_i P(A_i) \quad (2.5)$$

To get a lower bound, for $1 \leq k \leq m$, we write

$$P(\bigcap_{i=1}^k A_i) = P(A_1)P(A_2|A_1)P(A_3|A_1 \cap A_2) \dots P(A_k|\bigcap_{i=1}^{k-1} A_i).$$

Letting $C_{1j} = \{j\}$ $1 \leq j \leq k$ and $C_{2j} = \{1, 2, \dots, j-1\}$, $j = 1, 2, \dots, k-1$, $C_{20} = \phi$, we have, from (2.2), $P(A_j|\bigcap_{i=1}^{j-1} A_i) \geq P(A_j)$. Hence

$$P(\bigcap_{i=1}^m A_i) \geq \prod_{i=1}^m P(A_i). \quad (2.6)$$

In particular, if $P(A_i) = p$, $i = 1, 2, \dots, m$, then

$$p^m \leq P\left(\bigcap_{i=1}^m A_i\right) \leq p \quad (2.7)$$

and

$$\tilde{P}\left(\bigcap_{i=1}^m A_i\right) = p^{(m+1)/2}. \quad (2.8)$$

If, in a system of m components, k have identical failure distributions (they need not be physically identical), we refer to these components as being repeated components.

Example 2.2 Consider an m -component parallel system with m repeated components. Let A_i be the event that the i^{th} component fails. Then $P\left(\bigcap_{i=1}^m A_i\right)$ is the probability that the system fails and by the square root bounding method, we obtain (2.8). In particular, for $m = 2$, $\tilde{P}(A_1 \cap A_2) = p^{3/2}$. We subsequently examine this special case in substantially more detail.

In G. T. Edwards and I. A. Watson [7], a modification of (2.3) and (2.4) for k of m systems is given. This modification is based on an approximation to (2.3) and (2.4) which may be derived assuming low failure probabilities and employing the β -factor method, which is discussed in Section 3.

We describe this for 2 of 3 systems.

A 2 of 3 system fails if two or more components fail. If the failures of components are independent and identically distributed with failure probability p , then the probability that the system fails is

$$P = p^3 + 3p^2(1 - p). \quad (2.9)$$

Under the reasonable assumption that p is small,

$$p \sim 3p^2. \quad (2.10)$$

In Edwards and Watson, this is taken to be the lower bound \underline{p} , however, as is evident from (2.9), it is not a lower bound. The reasoning by which this is taken as the lower bound is not given in Edwards and Watson. We can nevertheless justify it as an approximation to the lower bound for small p , using some simplified mathematical models to describe common failures. One way to do this uses the beta factor model and will be treated in Section 3. The upper bound given by Edwards and Watson is $\bar{p} = p$, which is less than (2.9) for $1/2 < p < 1$ and less than (2.10) for $p > 1/3$.

The rationale given in WASH-1400 for the square root bounding method (2.4) may be summarized as follows:

Let $F_X(x)$ be the log-normal distribution and let x_α be the solution (in x) of $F_X(x) = \alpha$. Then $(x_\alpha x_{1-\alpha})^{1/2}$ is the median of the log-normal distribution, for every $0 < \alpha < 1$. In WASH-1400, [16, App. IV, p. 19], this is described by saying that "a log-normal was used with its median positioned at the center (geometric midpoint) of the range". In Edwards and Watson [7, p. 110], "these boundary values (i.e., (2.3)) define the range in which the true system failure probability lies and in the WASH-1400 study a log-normal probability distribution was assumed for the range of possible values. Where the common-mode failure probability was not predominant in a system reliability analysis a best estimate was obtained by calculating the median of the log-normal distribution. This is the geometric mean of the range."

Since the range of the log-normal distribution is $(0, \infty)$, the above statement does not have a precise interpretation as given. If it is modified as follows,

$$\lim_{\alpha \rightarrow 0} (x_{\alpha} x_{1-\alpha})^{\frac{1}{2}} = M,$$

then the median M is characterizable in this manner.

However, as stated in WASH-1400, the assumption that the upper and lower bound of the failure probabilities should be presumed to be symmetrically located tail probabilities of the log-normal distribution is a completely arbitrary assumption. There does not appear to be any logical basis for such an assumption, other than the mathematical convenience of being able to combine the bounds as in (2.4) for the purpose of obtaining a single value "midway" between the two bounds in a well-defined sense.

The use of the log-normal distribution to model the distribution of unknown probabilities is highly questionable. It is possible that a specific Bayesian model with a prior distribution for unknown probabilities and range $(0,1)$ might be approximated by a suitable log-normal distribution. The question of the errors introduced by such an approximation would then be a matter for sensitivity analysis and will not be specifically examined in this report.

The Lewis Report [11] was highly critical of the square root bounding model. For the purposes of this report, it is worthwhile to summarize the criticisms given in the Lewis report. The square root bounding method is described as follows therein.

The true system is too complex to calculate a failure probability. Consequently a simple model is needed. Let M denote a possible model and let $P(M)$ denote the failure probability calculated using this model M . Assume that the probability that a given class of models A is correct is representable by

$$Q(A) = \int_A dQ(M). \quad (2.11)$$

Then the failure probability

$$p = \int P(M) dQ(M), \quad (2.12)$$

or the mean probability with respect to the probability distribution $Q(M)$. In WASH-1400, $Q(M)$ is taken to be the log-normal distribution. Rather than attempting to characterize the set of possible models, in WASH-1400, two models, an upper bound model and a lower bound model are constructed. These are selected subjectively, presumably using engineering judgment. It is further assumed that these two models are symmetrically situated, resulting in the average \tilde{P} .

"The degree of arbitrariness in this procedure boggles the mind. The lower bound gives a bound which is so low as to be absurd, and there is no reason to believe that the upper bound is in any sense a symmetrically placed upper bound. Nor is there any reason to believe that $Q(M)$ is log-normal. The results are very sensitive to these arbitrary choices."

A somewhat similar critique of the square root bounding method is given by R. G. Easterling [6].

Assume that there is an event C such that $P(A_1 \cap A_2 | C)$ is the upper bound and $P(A_1 \cap A_2 | \bar{C})$ is the lower bound. Then

$$\tilde{P}(A_1 \cap A_2) = (P(A_1 \cap A_2 | C)P(A_1 \cap A_2 | \bar{C}))^{1/2}, \quad (2.13)$$

instead of

$$P(A_1 \cap A_2) = P(A_1 \cap A_2 | C)P(C) + P(A_1 \cap A_2 | \bar{C})P(\bar{C}), \quad (2.14)$$

a particular case of (2.12).

Somewhat more generally, let C_i , $i = 1, 2, \dots, N$ be a collection of such events. We suppose that the C_i 's are numerically valued and approximately log-normally distributed. Let C_5 and C_{95} be the lower and upper 5% points respectively. Then

$$(P(A_1 \cap A_2 | C_5)P(A_1 \cap A_2 | C_{95}))^{1/2} = \tilde{P}(A_1 \cap A_2) \quad (2.15)$$

and is asserted by R. G. Easterling to be the median of the distribution of $P(A_1 \cap A_2 | C_i)$. Easterling notes that this is not $P(A_1 \cap A_2)$ and also that

$$\sum_i P(A_1 \cap A_2 | C_i)P(C_i) = E\{P(A_1 \cap A_2 | C_i)\} \quad (2.16)$$

is the mean of the distribution ((2.14) is of course, the same as (2.12) with $P(M)$ replaced by $P(A_1 \cap A_2 | C_i)$). Easterling further notes that the mean of the log-normal distribution is larger than the median of the log-normal distribution.

First it should be noted that (2.12) and (2.16) are quite different assumptions than (2.4). Specifically, if M in (2.12) is log-normally distributed, this places little restriction on the distribution of $P(M)$. It is $P(M)$ and not $Q(M)$ that is assumed to be log-normally distributed in WASH-1400. While the log-normal distribution provides a weak justification for (2.4), one may still regard (2.4) as a convenient interpolation between two presumed extreme values. Thus it is of substantially greater interest to ascertain how (2.4) behaves and further to ascertain when it is a reasonable approximation.

For simplicity, we take $m = 2$. Let X_1, X_2 be two identically distributed Bernoulli random variables with $\rho(X_1, X_2) > 0$, where ρ denotes the correlation coefficient.

Then

$$P\{X_1 = 1, X_2 = 1\} = \rho p(1 - p) + p^2, \quad (2.17)$$

$$P\{X_1 = 1\} = P\{X_2 = 1\} = p. \quad (2.18)$$

The condition $\rho > 0$ is equivalent to (2.2), when $m = 2$ and $P(A_1) = P(A_2) = p$. This can be seen as follows

$$\rho = \frac{P\{X_1 = 1, X_2 = 1\} - p^2}{p(1 - p)}$$

from which, letting $A_1 = \{X_1 = 1\}$, $A_2 = \{X_2 = 1\}$, we have

$$P\{A_1|A_2\} = P\{A_2|A_1\} = (\rho p(1-p) + p^2)/p = \rho(1-p) + p \geq p,$$

with equality, if and only if $\rho = 0$.

The square root bounding method, as illustrated in (2.8) gives the estimate $p^{3/2}$ for this case.

Consequently, we examine

$$H_\rho(p) = (p^2 + \rho p(1-p))/p^{3/2}, \quad (2.19)$$

In particular, let α and β be two designated constants with $\alpha < 1$, $\beta > 1$.

The objective is to determine the set

$$D_\rho(\alpha, \beta) = \{p | \alpha \leq H_\rho(p) \leq \beta, \quad 0 \leq p \leq 1\}. \quad (2.20)$$

For $\rho = 0$, $H_0(p) = p^{1/2} < 1$, so that $H_0(p) \leq \beta$, $0 < p < 1$; $H_0(p) \geq \alpha$ holds whenever $p \geq \alpha^2$. Similarly, $H_1(p) = p^{-1/2} > 1$, so that $H_1(p) \geq \alpha$, $0 < p < 1$; $H_1(p) \leq \beta$ holds whenever $p \geq 1/\beta^2$. For $0 < \rho < 1$,

$$\alpha \leq H_\rho(p) \leq \beta$$

is equivalent to

$$\alpha p^{1/2} \leq (1-\rho)p + \rho \leq \beta p^{1/2}.$$

Let $u = p^{1/2}$

$$(1-\rho)u^2 - \beta u + \rho \leq 0 \quad (2.21)$$

$$(1-\rho)u^2 - \alpha u + \rho \geq 0 \quad (2.22)$$

Thus (2.21) holds whenever

$$\left(\frac{\beta - \sqrt{\beta^2 - 4\rho(1-\rho)}}{2(1-\rho)} \right)^2 \leq p < 1 \quad (2.23)$$

and (2.22) holds for all $0 < p < 1$ whenever $\alpha^2 \leq 4\rho(1-\rho)$. Otherwise (2.22) holds whenever

$$0 < p \leq (\alpha - \sqrt{\alpha^2 - 4\rho(1-\rho)}) / 2(1-\rho)^2 \quad (2.24)$$

and

$$((\alpha + \sqrt{\alpha^2 - 4\rho(1-\rho)}) / 2(1-\rho))^2 \leq p < 1. \quad (2.25)$$

In practice, one will often take $\alpha = 1/\beta$ and values of β suggested by the intended application in WASH-1400 are $\sqrt{10}$ and 10. These are natural due to the interest in measuring errors to orders of magnitude.

We can summarize these results for $\beta = \sqrt{10}$ and $\beta = 10$ as follows:

For $\beta = \sqrt{10}$, $\rho \geq .026$, (2.21) and (2.22) are satisfied for

$$D_p(\alpha, \beta) = \{ (\sqrt{10} - \sqrt{10 - 4\rho(1-\rho)}) / 2(1-\rho) \leq p < 1 \}.$$

For $\rho < .026$,

$$D_p(\alpha, \beta) = \{ (\sqrt{10} - \sqrt{10 - 4\rho(1-\rho)}) / 2(1-\rho) \leq p \leq (\sqrt{.1} - \sqrt{.1 - 4\rho(1-\rho)}) / 2(1-\rho) \} \\ \cup \{ ((\sqrt{.1} + \sqrt{.1 - 4\rho(1-\rho)}) / 2(1-\rho)) \leq p < 1 \} .$$

For $\beta = 10$, $\rho > .0025$,

$$D_{\rho}(\alpha, \beta) = \{(10 - \sqrt{100 - 4\rho(1-\rho)})/2(1-\rho) \leq p < 1\}.$$

For $\rho \leq .0025$,

$$D_{\rho}(\alpha, \beta) = \{(10 - \sqrt{100 - 4\rho(1-\rho)})/2(1-\rho) \leq p \leq (.1 - \sqrt{.01 - 4\rho(1-\rho)})/2(1-\rho) \\ \cup ((.1 + \sqrt{.01 - 4\rho(1-\rho)})/2(1-\rho) \leq p < 1\}.$$

For very small values of ρ , the lower level of $D_{\rho}(\alpha, \beta)$ is approximately $\rho/\sqrt{10}$ when $\alpha = \sqrt{1/10}$, $\beta = \sqrt{10}$ and $\rho/10$ when $\alpha = 1/10$, $\beta = 10$.

It is also worthwhile to estimate the difference between the two quantities, that is, consider

$$\Delta_{\rho}(p) = p^2 + \rho p(1-\rho) - p^{3/2}$$

for small values of p and small values of ρ . Specifically, let $\rho = cp^{\alpha}$, $0 \leq \alpha$. Then it is easily seen that as $p \rightarrow 0$,

$$\Delta_{\rho}(p) \sim \begin{cases} cp^{\alpha+1} & 0 \leq \alpha < 1/2 \\ (c-1)p^{3/2} & \alpha = 1/2, c \neq 1 \\ p^2 & \alpha = 1/2, c = 1 \\ -p^{3/2} & 1/2 < \alpha \end{cases} \quad (2.26)$$

Finally, note that the square root bounding method yields conservative estimates whenever $H_{\rho}(p) < 1$.

The above discussion was restricted to parallel (redundant) systems of two components. This can be extended to k of m systems, however, at a substantial increase in complexity, which may serve to obscure the conclusions.

3. The Beta Factor Model

The beta factor model is basically a parametrization of binomial or Poisson models in which the failures are divided into two classes, individual and common failures. β denotes the expected proportion of failures which are common failures.

Thus, for a Poisson process with intensity λ , we let λ_i denote the expected number of individual failures per unit time and let λ_c denote the expected number of common failures per unit time. Then

$$\lambda = \lambda_i + \lambda_c, \quad \beta = \lambda_c / \lambda, \quad 0 \leq \beta \leq 1. \quad (3.1)$$

A description of the beta factor model is given in Edwards and Watson [7]. The technique is due to Fleming [8] and is utilized in Dhillon and Proctor [5].

To apply the beta factor model to the life testing model for systems reliability, one may proceed as follows:

Let X_1, X_2, \dots, X_m be identically distributed random variables with

$$P\{X_i \geq x\} = e^{-\lambda x}, \quad x > 0. \quad (3.2)$$

$X_i, i = 1, 2, \dots, m$ is to be identified as the waiting time to failure of the i^{th} component of a system.

Example 3.1. Consider a parallel system of two components. If independent, the probability that the system does not fail on or before time T is

$$R(T) = 2e^{-\lambda T} - e^{-2\lambda T}, \quad \lambda > 0, \quad T > 0. \quad (3.3)$$

Let $P_I(T)$ be the probability that an individual failure of a specified component does not occur on or before T . It is assumed that individual failures are independent. Let $P_C(T)$ be the probability that a common failure does not occur before time T . Then

$$R(T) = P_C(T)\{(P_I^2(T)|P_C(T)) + (2P_I(T)(1 - P_I(T))|P_C(T))\}, \quad (3.4)$$

upon assuming that the individual failures are conditionally independent, given that no common failure has occurred. In Edwards and Watson [7], the further simplifying assumption that common failures and individual failures are independent is made, resulting in

$$R(T) = P_C(T)\{P_I^2(T) + 2P_I(T)(1 - P_I(T))\}, \quad (3.5)$$

Now using the beta factor model and simplifying, we get

$$R(T) = P_C(T)\{2P_I(T) - P_I^2(T)\}, \quad (3.6)$$

where

$$P_C(T) = e^{-\beta\lambda T}, \quad P_I(T) = e^{-(1-\beta)\lambda T}. \quad (3.7)$$

Thus

$$R(T) = 2e^{-\lambda T} - e^{-2\lambda T + \beta \lambda T} \quad (3.8)$$

If $\beta = 0$, that is, there are no common failures, then (3.8) reduces to (3.3). If $\beta = 1$, that is, all failures are common failures, then $R(T) = e^{-\lambda T}$, since both components act as a unit (single component).

This can be extended to more complicated systems at the cost of increased complexity. A simplified treatment is given in Edwards and Watson [7], where it is assumed that the only common failures are those in which all components fail, a somewhat stringent assumption. A model which does not require this assumption is described in Section 5.

In the engineering literature, it is customary to approximate life testing formulas by assuming that $\lambda T \rightarrow 0$, in which case (3.8) is approximated by

$$R(T) \sim 1 - \beta \lambda T \quad (3.9)$$

This reasoning is applied to the square root bounding model by Edwards and Watson [7]. In particular consider a 2 of 3 system. That is, a system which operates whenever two or more of the three components function. Then, from (3.5),

$$\begin{aligned} R(T) &= P_C(T) \{ 3 P_I^2(T) (1 - P_I(T)) + P_I^3(T) \} \\ &= e^{-\beta \lambda T} \{ 3 e^{-2(1-\beta)\lambda T} (1 - e^{-(1-\beta)\lambda T}) + e^{-3(1-\beta)\lambda T} \} \\ &= 3 e^{-(2-\beta)\lambda T} - 3 e^{-(3-2\beta)\lambda T} + e^{-(3-2\beta)\lambda T} \\ &= 3 e^{-(2-\beta)\lambda T} - 2 e^{-(3-2\beta)\lambda T} \end{aligned} \quad (3.10)$$

Naturally, for $\beta = 0$,

$$R(T) = 3e^{-2\lambda T} - 2e^{-3\lambda T}, \quad (3.11)$$

in agreement with (2.9) for $p = e^{-\lambda T}$. For $\beta = 1$,

$$R(T) = 3e^{-\lambda T} - 2e^{-\lambda T} = e^{-\lambda T}, \quad (3.12)$$

since there is effectively only one component.

Using the approximation obtained by letting $\lambda T \rightarrow 0$,

$$R(T) \sim 3(1 - (2 - \beta)\lambda T) - 2(1 - (3 - 2\beta)\lambda T) \sim 1 - \beta\lambda T \quad (3.13)$$

Note that for $\beta = 0$, the failure probability, $1 - R(T)$, does not have a nontrivial approximation given by (3.13). This can be rectified by utilizing the second order terms in (3.11), obtaining

$$R(T) \sim 1 + 3(4\lambda^2 T^2/2) - 2(9\lambda^2 T^2/2) = 1 - 3\lambda^2 T^2$$

so that

$$1 - R(T) \sim 3\lambda^2 T^2,$$

in agreement with (2.10).

4. The Common Load Model

T. Mankamo [12] proposed the following model. Assume that the m components have independent and identically distributed random resistances R_1, R_2, \dots, R_m . We denote the probability density function of these resistances by $f_R(x)$. A random stress S with probability density function $g_S(x)$ occurs. Then the event that exactly k of the components fail simultaneously, $k = 1, 2, \dots, m$ is given by

$$\{R_{[k]} < S \leq R_{[k+1]}\}, \quad (4.1)$$

where $R_{[1]} \leq R_{[2]} \leq \dots \leq R_{[m]}$ are the ordered resistances. S is presumed to be independent of R_1, R_2, \dots, R_m .

A given component is assumed to fail whenever $R < S$. Thus

$$P\{R < S\} = \int_0^\infty \int_0^y f_R(x) g_S(y) dx dy. \quad (4.2)$$

This may be written

$$\int_0^\infty F_R(y) g_S(y) dy = E_S(R), \quad (4.3)$$

where $F_R(y)$ is the cumulative distribution function of the resistance and $E_S(R)$ denotes the expected value of R computed with respect to the probability distribution of the stress.

It follows that the probability that k components fail when subjected to the random stress S is

$$P_m(k) = \int_0^\infty \binom{m}{k} (F_R(y))^k (1 - F_R(y))^{m-k} g_S(y) dy. \quad (4.4)$$

Mankamo illustrates this model under the assumption that both R and S are normally distributed and also under the assumption that both R and S have the log-normal distribution.

For the normal distribution model with parameters $\mu_R, \mu_S, \sigma_R^2, \sigma_S^2$, Mankamo proposed the quantity

$$\gamma_{RS} = (1 + \sigma_R^2/\sigma_S^2)^{-1} \quad (4.5)$$

as a measure of the dependence of component failures. A measure based on the relative size of the two variances is logical. If σ_R^2/σ_S^2 is very small, then all components will tend to fail simultaneously or function simultaneously after being subjected to the random stress S . If σ_R^2/σ_S^2 is large, then the knowledge that a given component has failed provides little information about the failures of other components. The particular form of γ_{RS} chosen by Mankamo has a range $0 \leq \gamma_{RS} \leq 1$, which presumably is found to be intuitively useful.

Mankamo suggests defining a parameter n_k by

$$P_m(k) = (P_m(1))^{n_k}. \quad (4.6)$$

This is an appealing parameterization, since it provides a number n_k which describes the "effective redundancy," or equivalently, $m - n_k$ describes the loss in redundancy due to common failures.

Mankamo says that the common load model is difficult to utilize when failure rates rather than failures on demand are involved. He suggests defining the probability of a common failure of k components by

$$P_k(T) = (1 - e^{-\lambda T})^{n_k}, \quad (4.7)$$

where n_k is determined by (4.6). The customary approximation (3.9) gives

$$P_k(T) \sim (\lambda T)^{n_k}. \quad (4.8)$$

5. The Binomial Failure Rate Model

This model was proposed by W. E. Vesely [18]. An extensive discussion of this model is given by C. L. Atwood [2]. A description of this model follows.

Let $U_i = 1$ if the i th component fails and 0 if the i th component functions, $i = 1, 2, \dots, n$. Then, the state of the system is given by a vector $\tilde{u} = (u_1, u_2, \dots, u_m)$, $u_i = 0, 1$. There are $2^m - 1$ possible outcomes in which one or more components fail simultaneously. For each \tilde{u} , let

$$f_{\tilde{u}}(t) = \lambda_{\tilde{u}} e^{-\lambda_{\tilde{u}} t}, \quad t > 0, \quad \lambda_{\tilde{u}} > 0 \quad (5.1)$$

be the probability density function of the waiting time for the failure combination \tilde{u} .

Let $w = \sum_{i=1}^m u_i$ be the weight of the vector \tilde{u} . Then define

$$\lambda_{\tilde{u}} = \begin{cases} m\lambda + \mu(mpq^{m-1}), & w(\tilde{u}) = 1, \\ \mu \binom{m}{i} p^i q^{m-i}, & w(\tilde{u}) = i > 1, \end{cases} \quad (5.2)$$

where $0 < p < 1$, $q = 1 - p$, $\lambda > 0$, $\mu > 0$, $m \geq 2$. Consequently, we simplify notation, writing $\lambda_{\tilde{u}} = \lambda_i$, $i = 1, 2, \dots, m$, where $i = w(\tilde{u})$.

Thus, for a parallel system of two components, the system fails by time T if either both of $(0,1)$ and $(1,0)$ occur or if the combination $(1,1)$ occurs. Thus the probability that the system fails is

$$(1 - e^{-\lambda_1 T})^2 + (1 - e^{-\lambda_2 T}) \sim (\lambda_1 T)^2 + \lambda_2 T, \quad (5.3)$$

the approximation being obtained using the reasoning employed in deriving (3.9). The common failure rate is

$$\lambda_+ = \sum_{i=2}^m \lambda_i. \quad (5.4)$$

A detailed discussion of this model and procedures for statistical estimation of the parameters may be found in C. L. Atwood [2]. The intuitive justification for the model (5.1) and (5.2) may be stated as follows. The individual components have a lifetime distribution determined by the exponential distribution with parameter λ . Shocks also arrive in accordance with a Poisson process with intensity μ . As each shock occurs, the individual components fail independently with probability p . From (5.3) we see that no provision is made for down time, that is, it is assumed that all failures are repaired instantly.

6. A Shock Model

G. Apostolakis [1] proposed the following model. Each of m components has an independent exponentially distributed life distribution with common parameter λ . In addition, shocks arrive in accordance with a Poisson process, stochastically independent of the above random lifetimes. This Poisson process has parameter λ_c and each shock induces the simultaneous failure of all m components. Thus, there are two possible modes of failure of a given set of $k \leq m$ components before a specified time T . The k components can fail individually, in accordance with the lifetime distribution or they can be subjected to a shock inducing a common failure. Thus, the reliability of a parallel system of k components is

$$R(T) = [1 - (1 - e^{-\lambda T})^k][e^{-\lambda_c T}]. \quad (6.1)$$

Similarly, for a k of m system,

$$R(T) = e^{-\lambda_c T} \sum_{r=k}^m \binom{m}{r} e^{-r\lambda T} (1 - e^{-\lambda T})^{m-r}. \quad (6.2)$$

Write

$$1 - \sum_{r=k}^m \binom{m}{r} e^{-r\lambda T} (1 - e^{-\lambda T})^{m-r} = \sum_{r=0}^{k-1} \binom{m}{r} e^{-r\lambda T} (1 - e^{-\lambda T})^{m-r}. \quad (6.3)$$

As $\lambda T \rightarrow 0$,

$$\begin{aligned} \sum_{r=0}^{k-1} \binom{m}{r} e^{-r\lambda T} (1 - e^{-\lambda T})^{m-r} &= \binom{m}{k-1} e^{-(k-1)\lambda T} (1 - e^{-\lambda T})^{m-k+1} (1 + O(\lambda T)) \\ &= \binom{m}{k-1} (\lambda T)^{m-k+1} (1 + O(\lambda T)). \end{aligned} \quad (6.4)$$

Thus as $\lambda_c T \rightarrow 0$,

$$R(T) \sim (1 - \lambda_c T)(1 - \binom{m}{k-1}(\lambda T)^{m-k+1}). \quad (6.5)$$

In this form, it is possible to determine how significant the probability of common failure is relative to the overall reliability. Apostolakis [1] gave a representation in terms of the hazard function of the k of m system lifetime.

7. A Suggested Common Failure Model.

The model described here was proposed by the author and is motivated by some of his work [3] on the stress-strength models in reliability. This model is an extension of the common load model of Mankamo [12, 13] and is also related to the binomial failure model, but is more fundamental than that model, in a probabilistic sense.

Specifically, the model is defined as follows.

Let $N(t)$ be the number of shocks arriving on or before t , $0 \leq t \leq T$. If $n(t)$ shocks have arrived in $[0, T]$, we designate the arrival times by $0 < t_1 < \dots < t_n < T$. The shocks are assumed to have random magnitudes $X(t_1), X(t_2), \dots, X(t_n)$; it is further assumed that $X(t_1), X(t_2), \dots, X(t_n)$ are independent and identically distributed. Consider a system of m components. To each component, we associate independent random variables Y_1, Y_2, \dots, Y_m . Component i is said to fail at time t_j whenever $X(t_j) > Y_i$, $i = 1, 2, \dots, m$. It is convenient to order (Y_1, Y_2, \dots, Y_m) , replacing them by the random variables $0 \leq Y_{[1]} \leq Y_{[2]} \leq \dots \leq Y_{[m]}$. Then, r components fail simultaneously at time t_j whenever

$$Y_{[r]} < X(t_j) \leq Y_{[r+1]}, \quad r = 0, 1, \dots, m, \quad (7.1)$$

where $Y_{[0]} = 0$, $Y_{[m+1]} = \infty$.

Within this structure, several specializations which are appropriate for a number of potential applications can be prescribed.

In some instances, one may wish to assume that $Y_{[1]}, Y_{[2]}, \dots, Y_{[m]}$ are known. This information may be obtained from non-destructive testing or from extensive knowledge of physical properties of the components. This model is closely related to the model described in J. D. Church and B. Harris [3].

Another modification of interest is the following. The random variables Y_i , $i = 1, 2, \dots, m$, which represent the strengths or resistances of the individuals components are subject to "wear out." This can be accomplished by defining a family of random functions $Y_i(t)$ $i = 1, 2, \dots, m$, where for $t_1 < t_2$, $Y_i(t_1) \leq Y_i(t_2)$ and $Y_i(t) \rightarrow 0$ as $t \rightarrow \infty$. The precise choice of these functions would require specific knowledge of the physical characteristics of the components.

Further, it may be appropriate to assume that the shocks have a degrading effect. That is, if they do not cause failure of a component, it may weaken that component so that the next shock will be more likely to induce a failure. This may be described by introducing functions as follows:

$$Y_i(t_j+) = H(Y_i(t_j), X(t_j)) , \quad (7.2)$$

where $Y_i(t_j+) \leq Y_i(t_j)$. To characterize the functions (7.2), engineering models for fatigue and shock damage are needed and such models will depend on the precise nature of the components.

Some specific illustrations follow.

Example 7.1. Assume that $Y_1 = y_1, Y_2 = y_2, \dots, Y_m = y_m$ are known and that the waiting times between shocks are independent exponentially distributed with common parameter λ . Assume further that $X(t_1), X(t_2), \dots, X(t_m)$ are independent identically distributed with probability density function

$$f_{(X)}(x) = \beta e^{-\beta x}, \quad x > 0, \quad \beta > 0.$$

With no loss of generality, we can assume $y_1 < y_2 < \dots < y_m$. Then let Z_j be the number of components failing at time t_j . Accordingly,

$$P\{Z_j = r\} = e^{-\beta y_r} - e^{-\beta y_{r+1}}, \quad r = 0, 1, \dots, m, \quad (7.3)$$

where $y_0 = 0, y_{m+1} = \infty$.

Then the probability of a common cause failure in $[0, T]$ is

$$P_c(T) = 1 - P(Z_1 \leq 1, Z_2 \leq 1, \dots) \quad (7.4)$$

In (7.4), there is a tacit assumption that failed components are "instantaneously" replaced or repaired. Thus,

$$\begin{aligned}
P_c(T) &= 1 - \sum_{j=0}^{\infty} P\{N(T) = j\} P\{X(t_i) \leq y_2, i = 1, 2, \dots, j\} \\
&= 1 - \sum_{j=0}^{\infty} \frac{(\lambda T)^j e^{-\lambda T}}{j!} (1 - e^{-\beta y_2})^j \\
&= 1 - \sum_{j=0}^{\infty} \frac{((\lambda T)(1 - e^{-\beta y_2}))^j}{j!} e^{-\lambda T} \\
&= 1 - e^{-\lambda T e^{-\beta y_2}}.
\end{aligned} \tag{7.5}$$

Thus, for this very special model, one does get a "nice" answer.

One can extend (7.4) and (7.5) easily to calculate the probability that i or more components fail simultaneously.

8. Concluding Remarks.

The present report described several possible models for common failures, one of which is believed to be new. With the exception of the square root bounding method, all appear to be plausible models and presumably can be regarded as approximations to reality on probabilistic grounds, under suitable physical conditions. Consequently, one now needs to extend the probabilistic models described herein to systems commonly encountered in practice. Then one should compare the models with existing data on common failures. Finally, statistical inference for these models needs to be studied. These investigations are to be considered in future reports.

REFERENCES

- [1] Apostolakis, G. E., Effect of a certain class of potential common mode failures on the reliability of redundant systems, *Nuclear Engineering and Design*, Vol. 36, 123-137.
- [2] Atwood, C. L., Estimators for the binomial failure rate common cause model, *NUREG/CR-1401*, 1980.
- [3] Church, J. D. and Harris, B., The estimation of reliability from stress-strength relationship, *Technometrics*, 12, (1970), 49-54.
- [4] Daniels, H. E., The statistical theory of the strength of bundles of threads, *Proc. Roy. Soc., London, Ser. A*, 183, (1945), 405-435.
- [5] Dhillon, B. S. and Proctor, C. L., Common mode failure analysis of reliability networks, *Proceedings, Reliability and Maintainability Symposium*, (1977), 404-408.
- [6] Easterling, R. G., Probabilistic analysis of "common mode failures". Vol. III, *Probabilistic Analysis of Nuclear Reactor Safety*, 1978, *Proceedings of Topical Meeting*, Newport Beach, California (1978).
- [7] Edwards, G. T. and Watson, I. A., A study of common mode failures, *United Kingdom Atomic Energy Authority*, 1979.
- [8] Fleming, K. N., A reliability model for common mode failures in redundant safety systems, *Modeling and Simulation*, Vol. 6, 6th Annual Conference, Pittsburgh, 1975, 579-581.
- [9] Fleming, K. N. and Raabe, Paul H. A comparison of three methods for the quantitative analysis of common cause failures, Vol. III, *Probabilistic Analysis of Nuclear Reactor Safety*, American Nuclear Society, 1978 (*Proceedings of Topical Meetings*, Newport Beach, California, 1978).
- [10] Gesellschaft für Reaktorsicherheit mbH, *Deutsche Risiko Studie-Kernkraftwerke*, Fachband 2/I, 1980.
- [11] Lewis, H. W., Chairman, Risk Assessment Review Group Report to the U. S. Nuclear Regulatory Commission, *NUREG/CR-0400*, 1978.
- [12] Mankamo, T., Common load model, A tool for common cause failure analysis, *Sähkötekniikan laboratorio*, Technical Research Centre of Finland, Tiedonanto 31, 1977.
- [13] Mankamo, T., Common cause failure of reactor pressure components, in *Reliability Problems of Reactor Pressure Components*, Vol. I, 125-136, International Atomic Energy Agency, Vienna 1978.
- [14] Sen, P. K., An asymptotically efficient test for the bundle strength of filaments, *J. Appl. Prob.*, 10, (1973), 586-596.

- [15] Sen, P. K., On fixed size confidence bounds for the bundle strength of filaments, Ann. Statist. Vol. 1, (1973), 526-537.
- [16] U. S. Nuclear Regulatory Commission, Reactor Safety Study, WASH-1400, Appendix IV, 1975.
- [17] U. S. Nuclear Regulatory Commission, P.R.A. Procedures Guide, NUREG/CR-2300, 1983.
- [18] Vesely, W. E., Estimating Common Cause Failure Probabilities in Reliability and Risk Analyses: Marshall-Olkin Specializations, in Nuclear Systems Reliability Engineering and Risk Assessment, J. B. Fussell, G. R. Burdick, Editors; SIAM, Philadelphia, 1977, 314-341.

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER 2659	2. GOVT ACCESSION NO. AD-A141490	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) STOCHASTIC MODELS FOR COMMON FAILURES OF COMPONENTS		5. TYPE OF REPORT & PERIOD COVERED Summary Report - no specific reporting period
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Bernard Harris		8. CONTRACT OR GRANT NUMBER(s) DAAG29-80-C-0041
9. PERFORMING ORGANIZATION NAME AND ADDRESS Mathematics Research Center, University of 610 Walnut Street Wisconsin Madison, Wisconsin 53706		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS Work Unit Number 4 - Statistics and Probability
11. CONTROLLING OFFICE NAME AND ADDRESS U. S. Army Research Office P.O. Box 12211 Research Triangle Park, North Carolina 27709		12. REPORT DATE March 1984
		13. NUMBER OF PAGES 29
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)		15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE
16. DISTRIBUTION STATEMENT (of this Report) Approved for public release; distribution unlimited.		
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)		
18. SUPPLEMENTARY NOTES		
19. KEY WORDS (Continue on reverse side if necessary and identify by block number) Common failures, dependent failures, common mode failures, common cause failures		
20. ABSTRACT (Continue on reverse side if necessary and identify by block number) Various models for common failures are described and characterized. In particular, a time dependent stress-strength (loading) model is given.		

END

FILMED

1971

ADAMK